SECURITY POLICY ON INTELLIGENCE INFORMATION IN AUTOMATED SYSTEMS AND NETWORKS

(Effective 4 January 1983) [1]

Pursuant to the provisions of the Director of Central Intelligence Directive (DCID) on the Security Committee, policy is herewith established for the security of classified intelligence information (hereafter referred to as intelligence) [2] processed or stored in automated systems and networks.

1. Applicability

The controls and procedures in these provisions and the attached Computer Security Manual shall be applied by all Intelligence Community agencies. Intelligence Community agencies which release or provide intelligence to contractors, consultants or other government departments or agencies shall ensure beforehand that the intended recipients agree to follow these controls and provisions in their own processing or storing of intelligence in automated systems and networks.

Senior Officials of the Intelligence Community (SOICs) [3] shall ensure that the controls and procedures in these provisions and the attached manual are incorporated in regulations on this subject issued by Intelligence Community agencies.

25X1

2. Responsibilities

Each SOIC or his designee is responsible for ensuring compliance by his/her respective organization, and any other organization for which he/she has security responsibility, with these provisions and the attached Computer Security Manual. However, only an SOIC may accredit an automated system or network for operation in the Compartmented Mode.

3. Policy

SOICs shall establish and maintain within their agencies formal computer security programs to ensure that intelligence processed or stored by automated systems

---

[1] These provisions supersede those in DCID 1/16, effective 6 June 1982. They derive from and have the force of the DCID on the Security Committee, effective 15 July 1982.

[2] For purposes of this policy statement, classified intelligence information ("intelligence") means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources or methods, that has been classified pursuant to Executive Order 12356 (or successor Order). "Foreign intelligence" and "counterintelligence" have the meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982 (or successor manual).

[3] Senior Officials of the Intelligence Community (SOICs), for purposes of these provisions, are the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives for intelligence matters.

and networks is adequately protected. The minimum security requirements for the allowed modes of operation of automated systems and networks are contained in the attached Computer Security Manual. Additional computer security measures may be established if deemed appropriate. Automated systems or networks shared with foreign governments shall be addressed on a case-by-case basis by the SOIC(s) involved in consultation with the DCI or his designee for this purpose.

4. Exceptions

25X1

[redacted]

Attachment:
DCI Computer Security Manual